

REMARKS

Claims 1-24 are pending in the Application.

Claims 1-24 stand rejected.

REJECTIONS UNDER 35 U.S.C. § 103

Claims 1-5, 8-13, 16-21, and 24 stand rejected under 35 U.S.C. § 103(a) as obvious over *Wu* (U.S. Patent No. 5,774,551). Claims 6-7, 14-15, and 22-23 stand rejected under 35 U.S.C. § 103(a) as obvious over *Wu* in view of *Savill* (Unix web article, dated December 10, 1999) Applicants respectfully traverse these rejections.

The basic test for nonobvious subject matter is whether the differences between the subject matter and the prior art are such that the claimed subject matter as a whole would not have been obvious to a person having ordinary skill in the art to which the subject matter pertains. The United States Supreme Court in *Graham v. John Deere & Co.*, 383 U.S. 1 (1966) set forth the factual inquiries which must be considered in applying the statutory test: (1) a determination of the scope and contents of the prior art; (2) ascertaining the differences between the prior art and the claims at issue; and (3) resolving the level of ordinary skill in the pertinent art.

Determining Scope and Content of Prior Art

In determining the scope and content of the prior art, the Examiner must first consider the nature of the problem on which the inventor was working. Once this has been established, the Examiner must select, for purposes of comparing and contrasting with the claims at issue, prior art references that are reasonably pertinent to that problem (the inventor's field of endeavor). See *Heidelberger Druckmaschinen AG v. Hantscho Commercial Products, Inc.*, 30 U.S.P.Q.2d 1377, 1379 (Fed. Cir. 1994). In selecting references, hindsight must be avoided at all costs.

The present invention relates to authentication and access within data processing systems. An application or operating system may support a sequence of logins. As part of the sequence of logins, a first security context is generated in response to a first authentication. The first authentication could include, for example, entry of a first user

ID and first password. As a further part of the sequence of logins, a second security context is generated in response to a second authentication. The second authentication could include, for example, entry of a second user ID and second password. The second security context aggregates the first security context and a security context corresponding to an identity in the second user authentication.

Wu teaches a system for achieving a unified login with a single authentication token to access numerous authentication services. To create a unified login, *Wu* discloses an application programming interface (also called "pluggable account management interface") that mediates between the system entry services and the account management services. *Wu*, col. 3, lines 10-14, 20-23. According to *Wu*, multiple authentication services may be used to increase the security of a computer system that supports various types of entry services such as a UNIX login, ftp, telnet, passwd, rlogin, and the like. See *Wu*, col. 1, lines 40-43, 49-52. *Wu* teaches separating the system entry services from the account management system so that use of account management services is transparent to the user and to the system entry services. *Wu*, col. 3, lines 1-7.

Savill is a brief web article that mentions the advantage of not closing all open applications and logging off. *Savill* discloses it is advantageous to have a utility that allows a user temporarily to start applications running in the security context of another account. See *Savill*, ¶ 1. *Savill* states that it is a good idea for system administrators to do some work with a low privileged account and only change to an account that is a member of the Administrators group if the system administrator really needs to do administrative work. *Savill* is scant on details, providing only a high level discussion of authentication utilities. *Savill* describes a utility that allows an administrator to run programs in the security context of any user in the system or domain. *Savill*, ¶ 3.

Differences Between Prior Art and Claims

The second step within the test described in *Graham* is to ascertain the differences between the cited prior art and the claims at issue. A *prima facie* showing of obviousness requires the Examiner to establish that the prior art references teach or suggest, either alone or in combination, all of the limitations of the claimed invention. The showings

must be clear and particular. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999).

Claim 1 recites:

1. An authentication method comprising the steps of:
generating a first security context in response to a first user authentication;
generating a second security context in response to a second user authentication, wherein said second security context aggregates said first security context and a security context corresponding to an identity in said second user authentication.

Wu fails to disclose every element of claim 1. For example, *Wu* does not disclose, "generating a second security context in response to a second user authentication." For this element, the Examiner cites the following sections from *Wu*:

However, in conventional systems where multiple authentication services are used to authenticate the user, the user must typically remember or provide an authentication token, for each authentication system. Authentication tokens include password, public keys, private keys, smart card personal identification numbers, biometric data such as retinal scans, fingerprints, voiceprint, and the like. *Wu*, col. 2, lines 8-14.

The system 100 further includes at least one account service 111. Each account service 111 includes methods that set and get account validation attributes, including authentication token aging information, such as when the authentication token expires, the maximum and minimum number of valid days, and the like; access hours restrictions for the user's account; account expiration date; and account service restrictions, such as what directories, file, resource, or services the user is authorized to access. Each account service 111 maintains these account validation attributes for each user's account, and provides methods to get and set this data on a per user basis. *Wu*, col. 17, lines 1-14.

Contrary to Examiner's assertions, the cited sections do not disclose the relevant elements of claim 1. Rather than disclosing generating a second security context in response to a second user authentication, *Wu* teaches generating a second security context in response to one, unified user authentication. See *Wu*, Col. 3, lines 11-14. Further, *Wu* teaches away from using a second user authentication. For example, *Wu* states the following when discussing multiple authentications:

This requirement typically makes it difficult for the user to access the system, especially where each authentication service has different requirements for allowable characters, length of key, age restrictions on keys, and other particular parameters. The use of multiple authentication tokens may be particularly difficult for novice users who are not familiar with the underlying system security policies or authentication services. Col. 2, lines 15-22.

Therefore, rather than teach a second user authentication, *Wu* teaches away by suggesting that a second user authentication may be particularly difficult for users. Therefore, *Wu* does not disclose, "generating a second security context in response to a second user authentication."

What is more, *Wu* fails to disclose other elements of claim 1. For example, *Wu* does not disclose, "wherein said second security context aggregates said first security context and a security context corresponding to an identity in said second user authentication." For these elements, the Examiner cites the following sections from *Wu*:

It is also desirable to provide a system and method where user is able to employ a single authentication token with any number multiple authentication services to obtain a unified login. It is finally desirable to provide a system to provide unified logout so that the user does not have to manually logout and destroy credentials created during the authentication process. *Wu*, col. 3, lines 11-14.

The pluggable account management interface 123 allows any system entry service 107 to be used transparently with any combination of account, password, session, or authentication services 109, including multiple instances of a given type of account management service. *Wu*, col. 6, lines 17-23.

The multiple authentication services 109 are illustrated in the figure. This process is used in support of the unified login, since the selected authentication services 109 have been determined transparently to the user. *Wu*, col. 17, lines 40-44.

Accordingly, the user is allowed to access the computer 101 only if authenticated by both of the services. *Wu*, col. 10, lines 33-35.

Finally, after the user has been authenticated, a session opened, and the user's account validated, the user is granted 325 access to the other services available on the computer system 100. *Wu*, col. 19, lines 54-56.

However, because *Wu* does not disclose a second user authentication, *Wu* necessarily cannot disclose "a security context corresponding to an identity in said second user authentication." Therefore, *Wu* does not disclose, "the second security context aggregates the first security context and a security context corresponding to an identity in the second user authentication."

The Examiner correctly recognizes that *Wu* does not recite every limitation of claim 1 by stating, "*Wu* does not teach the aggregated security context must be corresponding to an identity in second user authentication." Office Action, ¶ 5, Paper No. 5. However, despite *Wu*'s shortcomings, the Examiner states, "it would have been obvious" "to modify the unified login ID to be the identity of second user authentication because both of [the] login IDs are merely served as the unique identifiers." Office Action, ¶ 6, Paper No. 5. These statements are merely the Examiner's subjective opinions, unsupported by any facts or objective evidence. Further, even if the Examiner's statements are taken as true, the statements do not establish the obviousness of claim 1 because the Examiner fails to apply properly *Wu* to the language of claim 1. The Examiner essentially asserts that it would be obvious to modify *Wu*'s second security context (unified login ID) to be the identity of second user authentication. See Office Action, ¶ 6, Paper No. 5. However, claim 1 does not recite, "modify the second security context to be the identity of second user authentication." Therefore, *Wu* does not disclose "a security context corresponding to an identity in said second user authentication" and the Examiner has failed to show why one of ordinary skill in the art would modify *Wu* to practice claim 1.

Many principles disclosed in *Wu* and cited by the Examiner are fundamentally different from principles of the claims and specification of the present application. For example, *Wu* teaches a unified login that is specifically intended to avoid the need for both first and second user authentications. To the contrary, claim 1 recites a first and second user authentication. Further, *Wu* does not teach a method involving a first user authentication, a saving of the first security context, a second user authentication with the corresponding generation of a second security context (wherein the second security context aggregates the first security context and a security context corresponding to an

identity in a second user authentication), a log-off and then a reverting to the first security context. Instead, *Wu* essentially teaches a unified login that allows access to multiple systems without the need to provide login information more than once. In summary, *Wu* is fundamentally different from the subject matter of claim 1, *Wu* does not disclose every element of claim 1, and the Examiner has failed to provide adequate motivation to modify *Wu* to practice claim 1. Therefore, the Examiner has failed to establish a *prima facie* case that claim 1 is obvious over *Wu*. Consequently, claim 1 is patentable over *Wu* and *Savill*, taken alone or in combination.

Similarly, claim 2 is rejected as obvious over *Wu*. Claim 2 recites:

2. The method of claim 1 further comprising the step of saving said first security context.

In rejecting claim 2, the Examiner asserts that *Wu* teaches, "saving said first security context." Office Action, ¶ 7, Paper No. 5. In support, the Examiner cites from *Wu* "Unified login is accomplished through an authentication token mapping process." The cited text does not disclose saving the first security context; therefore, the Examiner has not established a *prima facie* case that claim 2 is obvious. MPEP § 2143.

Claim 3 is rejected as obvious over *Wu*. Claim 3 recites:

3. The method of claim 2 wherein said step of saving said first security context comprises the step of pushing said first security context on a stack.

In rejecting claim 3, the Examiner asserts that *Wu* teaches, "saving said first security context comprises the step of pushing said first security context on a stack." Office Action, ¶ 8, Paper No. 5. In support, the Examiner cites the following sections of *Wu*:

The ability to use multiple different ones of a given account management service is called "stacking," and it is particularly useful in conjunction with the authentication services. Col. 6, lines 64-67.

to be stacked for authenticating a user, and further enables unified login to such stacked authentication services 109 with a single password, and unified logout with a single logout command.

The cited section of *Wu* uses the words "stacking" and "stacked" however, the cited reference does not specifically disclose pushing the first security context on a stack

as part of the step of saving the first security context. Therefore, the Examiner has not established a *prima facie* case that claim 3 is obvious. MPEP § 2143.

The Examiner rejects claim 6 as obvious over *Wu* in view of *Savill*. Claim 6 recites:

6. The method of claim 2 further comprising the step of reverting to said first security context in response to a user logoff.

The Examiner states, "Savill teaches reverting to said first security context in response to a user logoff." The Examiner correctly recognizes that *Wu* does not disclose, "reverting to said first security context in response to a user logoff." Office Action ¶ 13, Paper No. 5. However, despite the Examiner's assertions, *Savill* does not disclose these elements either. *Savill* merely mentions the need for a Windows-based utility similar to the Unix-based "su" command. *Savill's* broad description of changing to an administrative account only when needed does not disclose every element of "reverting to said first security context in response to a user logoff" (emphasis added). *Savill* discloses that NTsu and SU.ZIP are available, but that an equivalent to "suid" is not available. *Savill* then describes "NTsu" briefly, disclosing that a user may have a desktop for each user and the user may switch from one desktop (and user) to another. Merely disclosing switching between desktops does not disclose, "reverting to said first security context in response to a user logoff." The only instance of *Savill* using the term "logoff" is in the context of the need to avoid closing all applications and logging off. See *Savill*, ¶ 1. Therefore, neither *Wu* nor *Savill* discloses, "reverting to said first security context in response to a user logoff." Therefore, claim 6 is not obvious over the cited references. MPEP § 2143.

Claim 7 is rejected as obvious over *Wu* in view of *Savill*. Claim 7 recites:

7. The method of claim 6 wherein said step of reverting to said first security context comprises the step of popping said first security context off of a stack.

The Examiner states "Savill further teaches reverting to said first security context comprises the step of popping said first security context off of a stack." Office Action, ¶ 16, Paper No. 5. Examiner's statement is erroneous because *Savill* does not teach popping the first security context off a stack. *Savill* does not disclose a stack and *Savill*

does not disclose popping any security context off a stack. Therefore, *Wu* and *Savill*, taken alone or in combination, do not disclose every limitation of claim 7. Consequently, claim 7 is not obvious over the cited references. MPEP § 2143.

Claims 1, 9, and 17 recite similar limitations and are rejected under the same reasoning. Office Action, ¶ 4, Paper No. 5. Therefore, the arguments made hereinabove for claim 1 also apply to show that claims 9 and 17 are not obvious over *Wu*.

Likewise, claims 2, 10, and 18 recite similar limitations and are rejected under the same reasoning. Office Action, ¶ 7, Paper No. 5. Therefore, the arguments made hereinabove for claim 2 also apply to show that claims 10 and 18 are not obvious over *Wu*. In addition, arguments made for claim 1 apply to show that *Wu* does not disclose every limitation of claims 2, 10, and 18.

Similarly, claims 3, 11, and 19 recite similar limitations and are rejected under the same reasoning. Office Action, ¶ 8, Paper No. 5. Therefore, the arguments made hereinabove for claim 3 also apply to show that claims 11 and 19 are not obvious over *Wu*. In addition, arguments made for claim 1 apply to show that *Wu* does not disclose every limitation of claims 3, 11, and 19.

Equally, claims 7, 15, and 23 recite similar limitations and are rejected under the same reasoning. Office Action, ¶ 16, Paper No. 5. Therefore, the arguments made hereinabove for claim 7 also apply to show that claims 15 and 23 are not obvious over *Wu* in view of *Savill*. In addition, arguments made for claim 1 apply to show that *Wu* does not disclose every limitation of claims 7, 15, and 23.

Also, claims 4, 5, and 8 depend directly or indirectly from claim 1. Therefore, claims 4, 5, and 8 recite the limitations of claim 1 and arguments hereinabove for the validity of claim 1 apply to claims 4, 5 and 8. Correspondingly, claims 12, 13, and 16 depend directly or indirectly from claim 10. Therefore claims 12, 13, and 16 recite the limitations of claim 10 and arguments hereinabove for the validity of claim 10 and claim 1 apply to claims 12, 13, and 16. In the same way, claims 20, 21, and 24 depend directly or indirectly from claim 17. Therefore claims 20, 21, and 24 recite the limitations of claim 17 and arguments hereinabove for the validity of claim 17 and claim 1 apply to claims 20, 21, and 24.

In summary, claims 1-24 are patentable over *Wu* and *Wu* in view of *Savill* because the references, alone or in combination, do not disclose every limitation of any claim. Therefore, claims 1-24 are allowable over *Wu* in view of *Savill* under 35 U.S.C. § 103. MPEP § 2143.

Ordinary Skill and Relevant Art

In resolving the level of ordinary skill of the pertinent art, as required by the third step in *Graham*, the Examiner must step backward in time and into the shoes worn by a person of ordinary skill when the invention was unknown and just before it was made. The hypothetical person skilled in the art can summarily be described as one who thinks along lines of conventional wisdom in the art and neither one who undertakes to innovate nor one who has the benefit of hindsight. Thus, neither an examiner, nor a judge, nor a genius in the art at hand, nor even the inventor is such a person skilled in the art.

The legal conclusion of obviousness must have a correct factual basis. See *Graham v. John Deere & Co.*, 383 U.S. 1 (1966); *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1455 (Fed. Cir. 1998). Where the legal conclusion is not supported by facts, it cannot stand. *Id.* A rejection based on § 103 clearly must rest on a factual basis, and these facts must be interpreted without hindsight reconstruction of the invention from the prior art. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). The patentability of an invention is not to be viewed with hindsight or "viewed after the event." *Goodyear Company v. Ray O Vac Company*, 321 U.S. 275, 279 (1944). The proper inquiry is whether modifying or bringing them together was obvious and not, whether one of ordinary skill, having the invention before him, would find it obvious through hindsight to construct the invention. Accordingly, an Examiner cannot establish obviousness by locating references that describe various aspects of the patent Applicant's invention without also providing evidence of the motivating force that would compel one skilled in the art to do what the patent applicant has done.

In order to establish a *prima facie* case of obviousness, it is necessary for the Examiner to present evidence, preferably in the form of some teaching, suggestion, incentive or inference in the applied prior art, or in the form of generally available

knowledge that one having ordinary skill in the art would have been led to modify or combine the relevant teachings of the applied references in the proposed manner to arrive at the claimed invention. *Ex parte Levengood*, 28 U.S.P.Q.2d 1300, 1301 (Bd. Pat. App. & Int. 1993); *Ashland Oil, Inc. v. Delta Resins and Refractories, Inc.*, 776 F.2d 281 (Fed. Cir. 1985). The motivation or suggestion to modify or combine references must come from one of three possible sources: the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. *In re Rouffet*, 47 U.S.P.Q.2d 1453, 1458 (Fed. Cir. 1998). The showings must be clear and particular. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). Broad conclusory statements regarding the teachings of multiple references, standing alone, are not evidence. *Id.*

The Examiner has not established a *prima facie* case of obviousness for rejecting claims 6-7, 14-15, and 22-23 because the Examiner has not cited sufficient motivation to combine *Wu* and *Savill*. The Examiner states as motivation: "*Savill* discloses a good idea from "Unix su" (substitute user or super-users) that allows the user to temporarily start applications running in the security context of a different account (e.g. first login as a regular user and subsequently login as the super-user for doing administrative work as a member of the administrators group) to avoid closing all open applications and log off all users." Office Action, ¶ 15, Paper No. 5. Stating that *Savill* discloses a good idea is not providing motivation to combine *Wu* with the teachings of *Savill* to practice the claimed invention. The Examiner has not presented evidence that one of ordinary skill in the art would combine the teachings. Therefore, the Examiner has not met his burden of showing motivation to combine *Wu* and *Savill*. Therefore, claims 6-7, 14-15, and 22-23 are allowable over *Wu* and *Savill*. MPEP § 2143.

Similarly, the Examiner fails to establish a *prima facie* case of obviousness by showing that one of ordinary skill in the art would be motivated to practice claim 1. The Examiner correctly recognizes that *Wu* does not disclose elements regarding the second security context, but then Examiner does not provide sufficient reason why one of ordinary skill in the art would modify *Wu* to practice claim 1. Office Action, ¶ 5-6, Paper No. 5. Instead, the Examiner provides a conclusory, insufficient motivation to modify, stating "It would have been obvious to the person of ordinary skill in the art at the time

the invention was made to modify the unified login ID to be the identity of second user authentication because both login IDs are merely served as the unique identifiers." The Examiner's stated motivation to modify fails to address the relevant claim elements. Further, the Examiner's stated motivation is merely the Examiner's subjective opinions, unsupported by any facts or objective evidence. Further, even if Examiner's statements are taken as true, the statements do not establish that one of ordinary skill in the art would be motivated to modify *Wu* to practice claim 1. Therefore, the Examiner's motivation to modify *Wu* to practice claim 1 is insufficient and claims 1-5, 8-13, 16-21, and 24 are allowable over *Wu*. MPEP § 2143.

As established above, the Examiner has not established a *prima facie* case that any claim is invalid over *Wu*, alone or in combination with *Savill*. However, even if the Examiner had met his burden, a *prima facie* case of obviousness may be rebutted by showing that the art teaches away from the claimed invention. *In re Geisler*, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997). *Wu*'s concept of unified login teaches away from having both a first user authentication and a second user authentication. Rather than disclosing such elements, *Wu* teaches away by disclosing, "The use of multiple authentication tokens may be particularly difficult for novice users who are not familiar with the underlying system security policies or authentication services." Col. 2, lines 19-22. Other ways in which *Wu* teaches away from the claimed subject matter are discussed in the above discussion of claim 1. Therefore, even if Examiner had established a *prima facie* case of invalidity of any claim, Applicants can rebut because *Wu* teaches away from having a first and second user authentication by teaching a unified login.

CONCLUSION

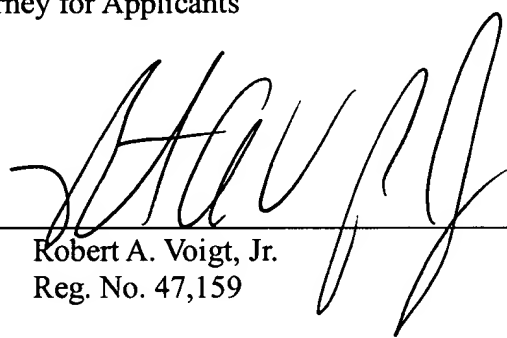
Wu and *Savill*, taken alone or in combination do not disclose every limitation of any of claims 1-24. There is no motivation to combine or modify the references to practice claims 1-24. The Examiner fails to establish a *prima facie* case that any claim is unpatentable over the cited references.

In consideration of the foregoing, all remaining claims are in condition for allowance. Applicants respectfully request an early allowance of such claims. Applicants respectfully request that the Examiner call Applicants' attorney at the below-listed number if the Examiner believes that such a discussion would be helpful in resolving any remaining issues.

Respectfully submitted,

WINSTEAD SECHREST & MINICK P.C.
Attorney for Applicants

By: _____


Robert A. Voigt, Jr.
Reg. No. 47,159

Kelly K. Kordzik
Reg. No. 36,571

P.O. Box 50784
Dallas, Texas 75201
(512) 370-2851